Theoretical Computer Science 7 (1978) 325–332

AN EXPLICIT CONSTRUCTION OF SHORT MONOTONE FORMULAE FOR THE MONOTONE SYMMETRIC FUNCTIONS

Mark KLEIMAN[1] and Nicholas PIPPENGER

Mathematical Sciences Department, IBM Thomas J. Watson Reasearch Center, Yorktown Heights, N.Y. 10598, U.S.A.

Communicated by Albert Meyer
Received November 1977

Abstract. We construct formulae that assume the value 1 when and only when at least k of their n variables assume the value 1, using only conjunction and disjunction, and having (for any fixed k) only

$$O\left((n \log n)\binom{k}{2}^{\log^* n}\right)$$

occurrences of variables.

1. Introduction

Let $x_1, \ldots, x_n$ be Boolean variables (assuming the values 0 and 1), and let $T_{k,n}(x_1, \ldots, x_n)$ be the Boolean function that assumes the value 1 when and only when at least k of these n variables assume the value 1. Our goal in this paper is to construct a formula for the function $T_{k,n}(x_1, \ldots, x_n)$ using the dyadic operations of conjunction (denoted $\wedge$) and disjunction (denoted $\vee$) and having a length (reckoned as the number of occurrences of variables) which is very nearly as small as possible. We shall restrict ourselves to the case in which k remains fixed while n increases.

By writing out the expansion

$$T_{n,k}(x_1, \ldots, x_n) = \bigvee_{1 \leq i_1 < \cdots < i_k \leq n} \bigwedge_{1 \leq s \leq k} x_{i_s},$$

we obtain a formula of length $O(n^k)$. For $k = 1$ this is $O(n)$, and is clearly the best possible. For $k = 2$ it is $O(n^2)$, but by using the identity

$$T_{2m,k}(x_1, \ldots, x_{2m}) = \bigvee_{0 \leq s \leq k} T_{m,s}(x_1, \ldots, x_m) \wedge T_{m,k-s}(x_{m+1}, \ldots, x_{2m})$$

[1] Permanent address: 164 Guyon Avenue, Staten Island, NY 10306, U.S.A.

recursively, Korobkov [7] has obtained a formula of length $O(n(\log n)^{k-1})$. (In this paper, log denotes the logarithm to the base 2, and ln denotes the natural logarithm, exp denotes the natural exponential.) For $k=2$, Korobkov's formula has length $O(n \log n)$. Krichevskii [8] has obtained a lower bound of $\Omega(n \log n)$ (which applies, in fact, for any $k \geq 2$) which shows that this is the best possible, even if the monadic operation of negation is also allowed. For $k=3$ Korobkov's formula has length $O(n(\log n)^2)$ and additional factors of $\log n$ appear for larger k. Khasin [4] has shown that for every fixed k there exist formulae of length $O(n \log n)$. Unfortunately, his proof does not exhibit a formula which meets this bound. For $k=3$, Khasin [5, 6] explicitly constructed a formula of length $O(n(\log n)^2/\log\log n)$ and, with the aid of negation, a formula of length $O(n(\log n)\log\log n)$. McColl and Paterson [9] constructed a formula of length $O(n(\log n)\log\log n)$ without the aid of negation, and with the aid of the dyadic operation of addition mod 2, they constructed a formula of length $O(n \log n)$. The last result cannot be compared with the lower bound $\Omega(n \log n)$, as the proof of the latter does not allow addition mod 2; only the much weaker lower bound $\Omega(n \log^* n)$ implicit in the work of Hodes and Specker [3] applies to these more general formulae. All of these constructions can be extended to larger values of k, but additional factors of $\log\log n$ (and eventually additional factors of $\log n$) appear.

In this paper we shall construct a formula of length

$$O\left((n \log n)\binom{k}{2}^{\log^* n}\right),$$

where log* is the very slowly growing function defined by

$$\log^* \xi = \begin{cases} 0 & \text{for } \xi \leq 1, \\ 1+\log^* \log \xi & \text{for } \xi > 1. \end{cases}$$

The profound torpidity of log* is evident from Fig. 1, where the next jump (to the value 6) occurs at an argument with 19,729 decimal digits. In particular, log* grows more slowly than all of the functions $\log^0, \log^1, \log^2, \ldots$, where $\log^0 \xi = \xi$ and $\log^{\nu+1} \xi = \log\log^\nu \xi$. Moreover, the base of the logarithms has relatively little effect: if $1 < \beta \leq 2$ and

$$\log_\beta^* \xi = \begin{cases} 0 & \text{for } \xi \leq 1, \\ 1+\log_\beta^* \log_\beta \xi & \text{for } \xi > 1, \end{cases}$$

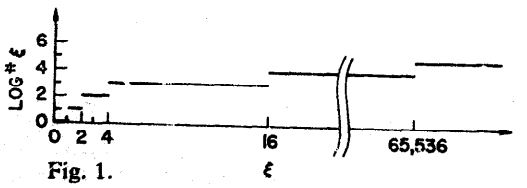

Fig. 1.

then it is an easy exercise to show that

$$\log^* \xi \leq \log^*_\beta \xi \leq \log^* \xi + L$$

for some constant L.

2. The construction

Consider a fixed integer $k \geq 2$. We shall construct a formula $F_n(x_1, \ldots, x_n)$ (the length of which will be denoted $f(n)$) for the function $T_{k,n}(x_1, \ldots, x_n)$ by means of a recursive process which will be applicable whenever n is sufficiently large, in a sense that will be made precise below. For the finitely many values of n that are not sufficiently large, any explicit construction will serve to terminate the recursion.

Let

$$\beta = \exp \frac{1}{k(k-1)}$$

and

$$Q(n) = \left[\left\{ 1 + \frac{1}{(\log^*_\beta n)^2} \right\} \binom{k}{2} \ln n \right].$$

For large n we have

$$Q(n) \sim \binom{k}{2} \ln n;$$

the very slowly decreasing multiplier

$$\left\{ 1 + \frac{1}{(\log^*_\beta n)^2} \right\}$$

is a "safety factor" whose purpose will become clear later.

For all *sufficiently large* n,

$$Q(n) \leq n - 1,$$

and thus we may apply this procedure recursively to construct a formula $F_{Q(n)}(y_1, \ldots, y_{Q(n)})$ for the function $T_{k,Q(n)}(y_1, \ldots, y_{Q(n)})$. Let $\eta_1, \ldots, \eta_{Q(n)}$ denote the numbers of occurrences of the variables $y_1, \ldots, y_{Q(n)}$ (respectively) in $F_{Q(n)}(y_1, \ldots, y_{Q(n)})$. Then

$$\sum_{1 \leq j \leq Q(n)} \eta_j = f(Q(n))$$

and we may assume without loss of generality (by reindexing the variables if necessary) that

$$\eta_1 \leq \cdots \leq \eta_{Q(n)}. \tag{1}$$

For each p $(1 \leq p \leq Q(n))$ and each j $(1 \leq j \leq Q(n))$, consider the formula

$$A_{p,j}(x_1, \ldots, x_n) = \begin{cases} \bigvee_{1 \leq i \leq n; i \equiv j \bmod p} x_i & \text{for } 1 \leq j \leq p, \\ 0 & \text{for } p+1 \leq j \leq Q(n). \end{cases}$$

The length of this formula is

$$a_{p,j} = \begin{cases} \left\lceil \dfrac{n+1-j}{p} \right\rceil & \text{for } 1 \leq j \leq p, \\ 0 & \text{for } p+1 \leq j \leq Q(n), \end{cases}$$

which satisfies

$$\sum_{1 \leq j \leq Q(n)} a_{p,j} = n$$

and

$$a_{p,1} \geq \cdots \geq a_{p,Q(n)}. \tag{2}$$

Let $B_p(x_1, \ldots, x_n)$ denote the formula obtained by substituting the formulae $A_{p,1}(x_1, \ldots, x_n), \ldots, A_{p,Q(n)}(x_1, \ldots, x_n)$ for the variables $y_1, \ldots, y_{Q(n)}$ (respectively) in the formula $F_{Q(n)}(y_1, \ldots, y_{Q(n)})$. The length of $B_p(x_1, \ldots, x_n)$ is

$$b_p = \sum_{1 \leq j \leq Q(n)} a_{p,j}\eta_j \leq \frac{1}{Q(n)} \left(\sum_{1 \leq j \leq Q(n)} a_{p,j} \right) \left(\sum_{1 \leq j \leq Q(n)} \eta_j \right) = \frac{n f(Q(n))}{Q(n)},$$

where we have exploited (1) and (2) by using Chebyshev's inequality (see [2, p.43, Theorem 43]).

Consider now the formula

$$F_n(x_1, \ldots, x_n) = \bigvee_{p \leq Q(n)} B_p(x_1, \ldots, x_n),$$

where p runs through the *primes* not exceeding $Q(n)$. Its length is

$$f(n) \leq \sum_{p \leq Q(n)} \frac{n f(Q(n))}{Q(n)}.$$

Let us show that $F_n(x_1, \ldots, x_n)$ is indeed a formula for the function $T_{k,n}(x_1, \ldots, x_n)$. It is obvious that $F_n(x_1, \ldots, x_n)$ implies $T_{k,n}(x_1, \ldots, x_n)$; we shall show that the converse implication holds as well. A typical term

$$\mathcal{C}(i_1, \ldots, i_k) = \bigwedge_{1 \leq s \leq k} x_{i_s}$$

in the expansion of $T_{k,n}(x_1, \ldots, x_n)$ will appear in the expansion of $B_p(x_1, \ldots, x_n)$ if the indices $i_1, \ldots, i_k$ have distinct residues mod p. This in turn will happen unless p divides the discriminant

$$\Delta(i_1, \ldots, i_k) = \prod_{1 \leq r < s \leq k} (i_s - i_r).$$

Thus the term $C(i_1, \ldots, i_k)$ will appear in the expansion of $F_n(x_1, \ldots, x_n)$ unless every prime p not exceeding $Q(n)$, and therefore also their least common multiple

$$E_{Q(n)} = \prod_{p \leq Q(n)} p,$$

divides the discriminant $\Delta(i_1, \ldots, i_k)$.

Now

$$E_{Q(n)} = \exp \theta(Q(n)),$$

where

$$\theta(\xi) = \sum_{p \leq \xi} \ln p.$$

Using the prime number theorem in the form

$$\theta(\xi) = \xi\left\{1 + O\left(\frac{1}{\ln \xi}\right)\right\}$$

(see [1, p.73, Theorem 6.2 and p.117, Problem 3(i)), and noting that any function $\lambda(n)$ of the form

$$\lambda(n) = \left\{1 + O\left(\frac{1}{\ln \ln n}\right)\right\}$$

satisfies

$$\left\{1 + \frac{1}{(\log_\beta^* n)^2}\right\}\lambda(n) \geq 1$$

for all *sufficiently large* n, we have

$$\theta(Q(n)) = \theta\left(\left\{1 + \frac{1}{(\log_\beta^* n)^2}\right\}\binom{k}{2} \ln n\right)$$

$$\geq \binom{k}{2} \ln n$$

and therefore also

$$E_{Q(n)} \geq n^{\binom{k}{2}}$$

for all sufficiently large n. Thus, since

$$1 \leq |\Delta(i_1, \ldots, i_k)| \leq (n-1)^{\binom{k}{2}},$$

no discriminant $\Delta(i_1, \ldots, i_k)$ can be divisible by $E_{Q(n)}$ and therefore no term $C(i_1, \ldots, i_k)$ can fail to appear in the expansion of $F_n(x_1, \ldots, x_n)$. This verifies that $F_n(x_1, \ldots, x_n)$ is a formula for the function $T_{k,n}(x_1, \ldots, x_n)$.

Let us now estimate $f(n)$ to complete the proof of our result. If we set

$$g(n) = \frac{f(n)}{n}$$

we have

$$g(n) \leq \sum_{p \leq Q(n)} g(Q(n)).$$

This can be written

$$g(n) \leq \pi(Q(n)) g(Q(n)),$$

where

$$\pi(\xi) = \sum_{p \leq \xi} 1.$$

Again using the prime number theorem, this time in the form

$$\pi(\xi) = \frac{\xi}{\ln \xi}\left\{1 + O\left(\frac{1}{\ln \xi}\right)\right\}$$

(see [1, p.47, Theorem A]), and noting that any function $\mu(n)$ of the form

$$\mu(n) = \left\{1 + O\left(\frac{1}{\ln \ln n}\right)\right\}$$

satisfies

$$\mu(n) \leq \left\{1 + \frac{1}{(\log_\beta^* n)^2}\right\}$$

for all *sufficiently large* n, we have

$$\pi(Q(n)) \leq \frac{\left\{1 + \frac{1}{(\log_\beta^* n)^2}\right\}^2 \binom{k}{2} \ln n}{\ln Q(n)}$$

and therefore also

$$g(n) \leq \frac{\left\{1 + \frac{1}{(\log_\beta^* n)^2}\right\}^2 \binom{k}{2} (\ln n)\, g(Q(n))}{\ln Q(n)},$$

for all sufficiently large n. If we set

$$h(n)=\frac{g(n)}{\ln n},$$

this can be written

$$h(n)\leqslant\left\{1+\frac{1}{(\log_\beta^* n)^2}\right\}^2\binom{k}{2}h(Q(n)).$$

This recurrence holds whenever n is sufficiently large, in the sense indicated by the three italicized occurrences of this phrase in the text above. For the finitely many values of n that are not sufficiently large we have

$$h(n)\leqslant H,$$

for some constant H.

By substituting the recurrence into itself w times we obtain

$$h(n)\leqslant\left(\prod_{0\leqslant v\leqslant w}\left\{1+\frac{1}{(\log_\beta^* Q^v(n))^2}\right\}^2\right)\binom{k}{2}^{w+1}h(Q^{w+1}(n)).$$

where $Q^0(n)=n$ and $Q^{v+1}(n)=Q(Q^v(n))$. Since

$$\left\{1+\frac{1}{(\log_\beta^* n)^2}\right\}\leqslant 2,$$

our choice of β implies

$$Q(n)\leqslant 2\binom{k}{2}\ln n=k(k-1)\ln n=\log_\beta n.$$

Thus for some w satisfying

$$w+1\leqslant\log_\beta^* n$$

we shall have

$$h(Q^{w+1}(n))\leqslant H$$

and

$$\binom{k}{2}^{w+1}\leqslant\binom{k}{2}^{\log_\beta^* n}$$

Furthermore since

$$Q(n)\leqslant\log_\beta n,$$

we have

$$\log_\beta^* Q^{v+1}(n)\leqslant -1+\log_\beta^* Q^v(n).$$

Thus the integers

$$\log_\beta^* Q^0(n), \log_\beta^* Q^1(n), \ldots, \log_\beta^* Q^w(n)$$

are distinct and

$$\prod_{0\le v\le w}\left\{1+\frac{1}{(\log_\beta^* Q^v(n))^2}\right\}^2 \le \prod_{1\le l<\infty}\left\{1+\frac{1}{l^2}\right\}^2 = O(1).$$

It follows that

$$h(n)=O\left(\binom{k}{2}^{\log_\beta^* n}\right),$$

$$g(n)=O\left((\log n)\binom{k}{2}^{\log_\beta^* n}\right),$$

and

$$f(n)=O\left((n\log n)\binom{k}{2}^{\log_\beta^* n}\right).$$

In view of the relation between $\log_\beta^*$ and $\log^*$, this completes the proof of the result.

References

[1] R. Ayoub, *An Introduction to the Analytic Theory of Numbers* (Amr. Math. Soc., Providence, RI, 1963).

[2] G.H. Hardy, J.E. Littlewood and G. Pólya, *Inequalities* (Cambridge Univ. Press, Cambridge, 1952).

[3] L. Hodes and E. Specker, Lengths of formulas and elimination of quantifiers, in: H.A. Schmidt, K. Schütte, and H.-J. Thiele, Eds., *Contributions to Mathematical Logic* (North-Holland, Amsterdam, 1968).

[4] L.S. Khasin, Otsenka slozhnosti realizatsii monotonnykh simmetrich eskikh funktsii formulami v bazise $\vee, \&, \neg$, *Dokl. Akad. Nauk SSSR* **189** (1969) 752–755, transl. as: Complexity bounds for the realization of monotonic symmetrical functions by means of formulas in the basis $\vee, \&, \neg$, *Soviet Physics Dokl.* **14** (1970) 1149–1151.

[5] L.S. Khasin, O realizatsii monotonnykh simmetricheskikh funktsii formulami v bazise $\vee, \&, \neg$, *Problemy Kibernet.* **21** (1969) 253–257, transl. as: On realizations of monotonic symmetric functions by formulas in the basis $\vee, \&, \neg$, *Systems Theory Res.* **21** (1969) 254–259.

[6] L.S. Khasin, Ob ispolzovanii otritsaniya dlya realizatsii monotonnykh simmetricheskikh funktsii algebry logiki formulami v bazise $\vee, \&, \neg$, *Diskret. Analiz* **17** (1970) 45–55.

[7] V.K. Korobkov, Realizatsiya simmetricheskikh funktsii v klasse Π-skhem, *Dokl. Akad. Nauk SSSR* **109** (1956) 260–263.

[8] R.E. Krichevskii, Slozhnost kontaktnykh skhem, realizuyushchikh odnu funktsiyu algebry logiki, *Dokl. Akad. Nauk SSSR* **151** (1963) 803–806, transl. as: Complexity of contact circuits realizing a function of logical algebra, *Soviet Physics Dokl.* **8** (1964) 770–772.

[9] W.F. McColl and M.S. Paterson, personal communications (1975–1977); see also W.F. McColl, Some results on circuit depth, University of Warwick Theory of Computation Report 18 (March 1977) 116–127.